(1)

a) $\sigma = (123)(45678)$ $\quad sgn(\sigma) = (-1)^2(-1)^4 = +1 \Rightarrow \sigma \in A_8$

Soit $\gamma = \gamma_1 \circ \cdots \circ \gamma_r$ une écriture de $\gamma \in S_8$ comme produit de cycles disjoints

Alors $|\gamma| = ppcm |\gamma_i|$ L'ordre plus grand pour un élément de S_8 est donc 15

b) Un anneau principal est un anneau commutatif intègre tel que tout idéal est engendré par un seul élément

$\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}/_{3\mathbb{Z}}[x]$ sont 3 anneaux principaux, le dernier de caractéristique 3

Ils sont tous euclidiens.

$\mathbb{Z}[x]$, $K[x,y]$, $\mathbb{Z}[i\sqrt{5}]$ sont des exemples d'anneaux com. intègres non principaux.

c) OUI Le lemme chinois nous dit que

$$m \wedge n = 1 \Rightarrow \varphi : \mathbb{Z}/_{mn\mathbb{Z}} \to \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$
$$c + mn\mathbb{Z} \mapsto (c + m\mathbb{Z}, c + n\mathbb{Z})$$

est un isomorphisme d'anneaux. En particulier $\forall a, b \in \mathbb{Z}$ il existe (unique modulo mn) $x \in \mathbb{Z}$ t.q. $x \equiv a \mod m$ et $x \equiv b \mod n$.

d) $\mathbb{Z} \subseteq A \subseteq \mathbb{Q} \Rightarrow Frac(\mathbb{Z}) \subseteq Frac(A) \subseteq Frac(\mathbb{Q}) \Rightarrow Frac(A) = \mathbb{Q}$.

$$Frac(\mathbb{Z}) = \mathbb{Q}, \quad Frac(\mathbb{Q}) = \mathbb{Q}$$

e) $2 + (x^2+1) = (1 - x + (x^2+1))(1 + x + (x^2+1))$ égalité dans $\dfrac{\mathbb{Z}[x]}{(x^2+1)}$

[Rmq l'application $\mathbb{Z}[x] \to \mathbb{Z}[i]$, $p(x) \mapsto p(i)$ induit un isomorphisme $\dfrac{\mathbb{Z}[x]}{(x^2+1)} \simeq \mathbb{Z}[i]$

donc il suffit de penser à $2 = (1+i)(1-i)$ dans $\mathbb{Z}[i]$]

(2) a) $A = \mathbb{Z}/5\mathbb{Z}[x]$ est euclidien Soit $t \in A$ $\deg t = 2$

Alors $\exists\, q, r \in A$ tt $a = tq + r$ avec

$r = \alpha x + \beta$ $\exists\, \alpha, \beta \in \mathbb{Z}/5\mathbb{Z}$

On a donc $|A/I| = |A/J| = 25$.

b) $x^2+1 = (x-2)(x-3)$ dans A

donc $(x-2+\bar{J})(x-3+\bar{J}) = \bar{J}$ dans A/J

c) Par le thm de correspondance les idéaux de A/J sont les B/J

avec B idéal de A qui contient J. Les possibles B sont donc

(en sachant que A euclidien $\Rightarrow A$ principal)

$B = A$ $B = J$ $B = (x-2)$ $B = (x-3)$

d) L'application $\varphi : A \longrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est un morphisme

$a(x) \longmapsto (a(2), a(3))$

d'anneaux surj de $\ker = \bar{J}$. Il suffit donc d'appliquer le thm d'iso.

Sinon soit $B_1 = (x-2)$ $B_2 = (x-3)$ alors $B_1 \cap B_2 = ((x-2)(x-3)) = J$

et $\begin{cases} A/J \simeq A/B_1 \times A/B_2 \\ a+J \mapsto (a+B_1,\ a+B_2) \end{cases}$ Il reste à prouver que

$A/B_1 \simeq \mathbb{Z}/5\mathbb{Z} \simeq A/B_2$ Par exemple $A \to \mathbb{Z}/5\mathbb{Z}$

$a(x) \mapsto a(2)$

est un morph. surj de kernel égal à $(x-2) = B_1$. On utilise le thm d'iso.

e) NON x^2+2 irred. dans A $\Rightarrow$ $A/_{(x^2+2)} = A/_I$ est un corps

donc sans diviseurs de zero

b) $a+I = (x+I)(x+1+I)^{-1}$

$x^2+2 = (x+1)(x-1)+3$ $\Rightarrow (x+1+I)^{-1} = 2(1-x)+I$

et $a+I = (x+I)(2(1-x)+I) = 2x+4+I$

(3) a) il faut m.q. $1 \in A$ et $\forall f,g \in A$ $f-g$ et $f\cdot g \in A$

si $f = \sum a_i x^i$ $g = \sum b_i x^i$ il faut donc al.p.

$3 \mid a_1, b_1$
$9 \mid a_2, b_2$
$\Rightarrow$ $\begin{cases} 3 \mid a_1 - a_2, & 9 \mid a_2 - b_2 \\ 3 \mid a_0 b_1 + a_1 b_0, & 9 \mid a_2 b_0 + a_1 b_1 + a_0 b_2 \end{cases}$

ce qui est evident

b) $27x^3 = (3x)(3x)(3x) = (3)(3)(3)(x^3)$

avec $3x$, 3, x^3 irred. dans A

c) A n'est pas factoriel car $27x^3$ ne peut pas s'ecrire de façon unique comme produit d'irred.

d) $(9x^2) \wedge (3x) = (9x^2)$ donc le ppcm de $9x^2$ et $3x$ est $9x^2$

par contre $\neq$ le ppcm de $9x^2$ et 3 en effet

$27x^2 = (9x^2)(3)$

$27x^3 = \begin{cases} (9x^2)\cdot(3x) \\ (3^3)\, x^3 \end{cases}$

donc $27x^2$ et $27x^3$ sont des multiples de 3 et $9x^2$. En plus $27x^2$ est le mult. de 3 et $9x^2$ de degré le plus petit

mais $27x^2 \nmid 27x^3$

(4) a) $U(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \wedge n = 1 \}$

$\Rightarrow |U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$

Thm Lagrange $\Rightarrow \forall \bar{x} \in U(\mathbb{Z}/n\mathbb{Z})$ $\quad \bar{a}^{|U(\mathbb{Z}/n\mathbb{Z})|} = \bar{1}$

$\Rightarrow \forall a \in \mathbb{Z}$ $a \wedge n = 1$ $\quad a^{\varphi(n)} \equiv 1 \mod n$.

b) $\varphi(25) = 20 = |\{ a \in \mathbb{N} \setminus \{0\} \mid a < 25 \}| - |\{5, 10, 15, 20\}|$

$2 \wedge 25 = 1$ donc (par a) $2^{20} \equiv 1 \mod 25$

Il suffit donc de vérifier que $\bar{2}^{-2} \neq 1$, $\bar{2}^4 \neq 1$, $\bar{2}^5 \neq 1$, $\bar{2}^{10} \neq \bar{1}$

pour conclure que $|\bar{2}| = 20$.

c) $\bar{2} \in U(\mathbb{Z}/25\mathbb{Z})$ $\quad |\bar{2}| = 20 = |U(\mathbb{Z}/25\mathbb{Z})|$ $\quad = \langle \bar{2} \rangle$ est un sous gp qui a le même cardinal du gp

$\Rightarrow \langle \bar{2} \rangle = U(\mathbb{Z}/25\mathbb{Z})$

d) $U(\mathbb{Z}/25\mathbb{Z})$ est cyclique de card. 20 $\Rightarrow$ il y a $\varphi(20) = 8$ éléments d'ordre 20

e) l'application

$$\{ n \in \mathbb{N}^{*} \mid n \mid 20 \} \longrightarrow \{ \text{sous gps de } U(\mathbb{Z}/25\mathbb{Z}) \}$$

$$n \longmapsto \langle \bar{2}^n \rangle$$

est inj. Les sous gps de $U(\mathbb{Z}/25\mathbb{Z})$ sont donc

$\langle \bar{2} \rangle = U(\mathbb{Z}/25\mathbb{Z})$, $\langle \bar{2}^2 \rangle$, $\langle \bar{2}^4 \rangle$, $\langle \bar{2}^5 \rangle$, $\langle \bar{2}^{10} \rangle$,

$\langle \bar{2}^{20} \rangle = \{ \bar{1} \}$.